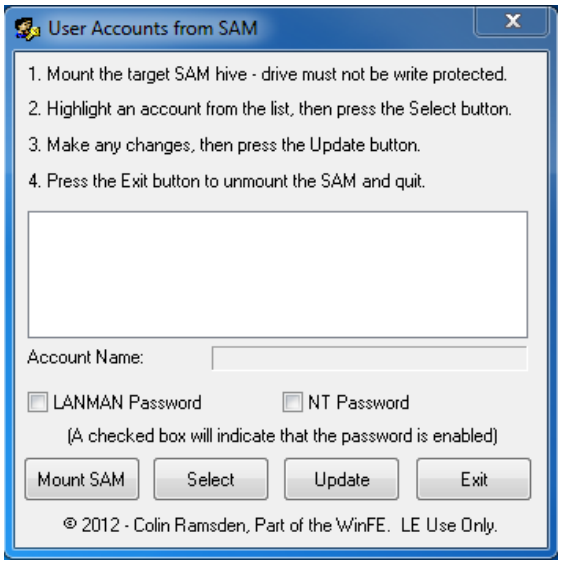
Password Removal Tool – User Guide

This tool should be used from the Windows Pre-Installation Environment (WinPE) or Windows Forensic Environment (WinFE).

If the tool is used from WinFE, the drive that contains the SAM hive file should be MOUNTED and set to READ-WRITE.

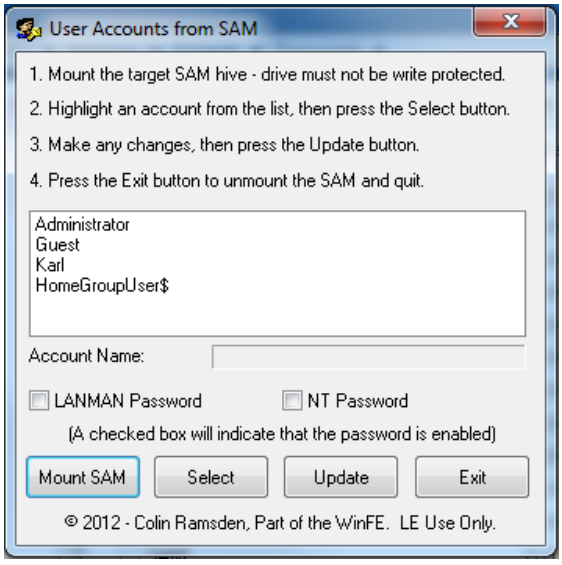
NOTE: This is not a forensically sound tool.

1, Run the PassKill.exe executable.


User Accounts from SAM
1. Mount the target SAM hive - drive must not be write protected.
2. Highlight an account from the list, then press the Select button.
3. Make any changes, then press the Update button.
4. Press the Exit button to unmount the SAM and quit.
Account Name:
LANMAN Password
NT Password
(A checked box will indicate that the password is enabled)
Mount SAM
Select
Update
Exit
© 2012 - Colin Ramsden, Part of the WinFE. LE Use Only.

2, Click the ‘Mount SAM’ button, then navigate to the location of the SAM hive, which is usually <Suspect Drive Letter>\Windows\System32\Config, then select the SAM hive file.

3, The list box should now be populated with all of the user accounts present for that installation of Windows.


User Accounts from SAM
1. Mount the target SAM hive - drive must not be write protected.
2. Highlight an account from the list, then press the Select button.
3. Make any changes, then press the Update button.
4. Press the Exit button to unmount the SAM and quit.
Administrator
Guest
Karl
HomeGroupUser$
Account Name:
LANMAN Password
NT Password
(A checked box will indicate that the password is enabled)
Mount SAM
Select
Update
Exit
© 2012 - Colin Ramsden, Part of the WinFE. LE Use Only.

4, Highlight the user account name you wish to check the password status for, then click the ‘Select’ button. As can be noted for the account ‘Karl’, there is an NT Password protecting the account (Indicated by the checked box).

User Accounts from SAM
1. Mount the target SAM hive - drive must not be write protected.
2. Highlight an account from the list, then press the Select button.
3. Make any changes, then press the Update button.
4. Press the Exit button to unmount the SAM and quit.
Administrator
Guest
Karl
HomeGroupUser$
Account Name:
Karl
LANMAN Password
NT Password
(A checked box will indicate that the password is enabled)
Mount SAM
Select
Update
Exit
© 2012 - Colin Ramsden, Part of the WinFE. LE Use Only.

5, To remove the password, simply uncheck the box(es), then click the ‘Update’ button.

6, Repeat this process for each account that you wish to remove the password from.

7, When finished, click the ‘Exit’ button, this is very important as the SAM hive is dismounted by this action.

8, The passwords can be reapplied, should it be required, by re-checking the boxes that were un-checked.